10 DEC 20041



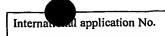


## **PCT**

## INTERNATIONAL PRELIMINARY EXAMINATION REPORT

ansi	PCT	•			
PATENT COOPERATION TREATY  PCT//B2003  PCT  INTERNATIONAL PRELIMINARY EXAMINATION REPORT  (PCT Articlé 36 and Rule 70)					
	(PCT Article 36 and	d Rule 70)			
Applicant's or agent's file reference P-14-418-PCT	FOR FURTHER ACTION	See Notification of Transmittal of Internal Preliminary Examination Report (Form PCT/IPEA)			
International application No. PCT/IB2003/002425	International filing date (day/n 10 June 2003 (10.06				
International Patent Classification (IPC) or H04L 9/08, H04N 7/16	national classification and IPC				
Applicant	NAGRACARD	SA			
Authority and is transmitted to the  2. This REPORT consists of a total o  This report is also accomp been amended and are the (see Rule 70.16 and Section	applicant according to Article 36  f 4 sheets, includi  anied by ANNEXES, i.e., sheets basis for this report and/or sheets on 607 of the Administrative Instr	ing this cover sheet.  of the description, claims and/or drawings which have sometimes containing rectifications made before this Authority			
These annexes consist of a  3. This report contains indications rel	ating to the following items:				
Basis of the repo	rt				
II Priority  III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability					
IV Lack of unity of					
V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability citations and explanations supporting such statement					
VI Certain documen	VI Certain documents cited				
· · · · · · · · · · · · · · · · · · ·	the international application				
VIII Certain observati	ions on the international applicati	ion			
Date of submission of the demand	Date of	of completion of this report			
20 December 2003 (20.	12.2003)	07 June 2004 (07.06.2004)			
Name and mailing address of the IPEA/EP	1	rized officer			
P.B. 5818 Patentlaan 2/ NL-2280 HV Tel. +31 70 340-2040	√ Rijswijk	Holper, G			
Facsimile No. +31 70 340-3016	Telent	hone No. +31 70 340-2304			

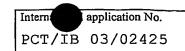




PCT/IB2003/002425

I. Basis of the report								
<ol> <li>This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):</li> </ol>								
$\boxtimes$	the international	application as originally filed.						
$\boxtimes$	the description,	pages, as originally filed,						
		pages, filed with the demand,						
		pages, filed with the letter of,						
		pages, filed with the letter of						
	the claims,	Nos1-16, as originally filed,						
الحا		Nos, as amended under Article 19,						
		Nos, filed with the demand,						
		Nos, filed with the letter of,						
		Nos, filed with the letter of						
$\boxtimes$	the drawings,	sheets/fig1/2-2/2, as originally filed,						
		sheets/fig, filed with the demand,						
		sheets/fig, filed with the letter of,						
		sheets/fig, filed with the letter of						
2. The amend	ments have result	ed in the cancellation of:						
	the description,	pages						
	the claims,	Nos						
	the drawings,	sheets/fig						
	<b></b> ,							
3. This to go	report has been e	stablished as if (some of) the amendments had not been made, since they have been considered osure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).						
""	o oo, and me also.							
4. Additional	observations, if n	ecessary:						
		·						
ł								
		•						

## INTERNATIONAL PREL. NARY EXAMINATION REPORT



v.	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability;
	citations and explanations supporting such statement

1.	Statement			
	Novelty (N)	Claims	1-16	YES
		Claims		NO
1	Inventive step (IS)	Claims	1-16	YES
		Claims		NO NO
	Industrial applicability (IA)	Claims	1-16	YES
		Claims		NO

2. Citations and explanations

Reference is made to the following document:

D1: WO 97/38530 (DIGCO)

The present application relates to a method for securely exchanging data between two locally mutually connected devices and a receiver for implementing said method.

The closest prior art is D1, which discloses a method for securely exchanging data between a receiver and a security module, wherein the two devices are locally connected. The receiver comprises a public key whereas the security module comprises a corresponding private key. The method is used for exchanging a random session key encrypted by means of the public key.

In the prior art, a problem arises in that an intruder can force the session key and thereby exploit a lack of security of the method.

According to claim 1, this problem is solved by the steps of generating a different random number in each device, encrypting this number by means of the first and second keys of the pair of keys respectively, transmitting the

## INTERNATIONAL PRELAMINATION REPORT



encrypted number to the other device, decrypting the numbers encrypted in each device and combining said random numbers to generate a session key used for exchanging data between the two devices.

A method based on the encryption of two random numbers encrypted by means of two separate keys from the same pair of keys is neither known from, nor suggested by, the prior art. Claim 1 therefore meets the requirements of novelty and inventive step of PCT Article 33(2) and (3).

The receiver according to claim 15 is used for implementing the method according to claim 1 and therefore also meets the requirements of novelty and inventive step.

The additional features of dependent claims 2 to 14 and 16 define details of the embodiment of the invention; said claims are therefore also novel and inventive.

The claimed methods and receivers are industrially applicable.

